Ilyesse El Adaoui

Travail à Faire

1

Objectif de la veille	Dégager de nouveaux procédés ou matériaux de substitution	Suivre les évolutions techniques	Identifier les meilleurs pratiques	Réaliser des projets personnels	Augmenter la qualité des produits	Anticiper la concurrence
Sources d'info	Crédibilité de l'auteur	Fiabilité de la source	Objectivité	Exactitude de l'information	actu de l'info	Pertinence de l'information
Exemple : site web	Le Monde Informatique : actualités, dossiers et tendances IT	Espacenet – recherche de brevets	Developpez.com, le club des développeurs et IT Pro	Accueil - LinuxFr.org	Office des brevets et des marques des États-Unis d'Amérique (uspto.gov)	Réseaux sociaux
Evaluation	4	4	4	4	3	2

2)

	Outil de collecte de l'info	Outil de traitement de l'information	Outil de curation de l'information	Outil de partage des résultats
Nom de l'outil	google alerts	Excel	Feedly	Réseaux sociaux
Avantages	Informé régulièrement des nouveautés sur le sujet de la veille	Accessible, gain de temps, traitement de données rapide	Les informations sont triées et classées c'est un gain de temps	Rapide, accessible

Inconvénients	Masse d’informations difficile à traiter	Nécessite une certaine connaissance		Pas toutes les données

3) Nessus : un outil d'analyse de vulnérabilité de système d'exploitation, de réseau et de périphérique qui permet de détecter les faiblesses de sécurité et les vulnérabilités de sites web. Il peut également générer des rapports détaillés sur les vulnérabilités détectées.

OWASP ZAP (Zed Attack Proxy): C'est un outil open-source pour l'analyse de sécurité des applications web. Il permet de détecter les vulnérabilités de sécurité telles que les injections SQL, les attaques par cross-site scripting (XSS) et les faiblesses de sécurité dans les paramètres d'authentification.

5) La solution que nous avons retenue est OWASP ZAP (Zed Attack Proxy), un outil open-source pour l'analyse de sécurité des applications web. Il permet de détecter les vulnérabilités de sécurité telles que les injections SQL, les attaques par cross-site scripting (XSS) et les faiblesses de sécurité dans les paramètres d'authentification. En utilisant cet outil, nous pouvons assurer à nos clients que nous prenons toutes les mesures nécessaires pour protéger leurs données et maintenir l'intégrité de notre site. Nous vous invitons à inclure cette information dans le prochain courrier que vous enverrez à nos clients pour les informer de cette nouvelle mesure de sécurité.